CYBERARK®

Cyber Hygiene Program

Cybercriminals steal $81 million from central bank

BREACH OVERVIEW	
Target	Bangladesh Central Bank
Attacker	Unknown
Motivation	Monetary
Outcome	$81M stolen and unrecovered

May 15, 2015:
Three bank accounts are opened at RCBC

January 29:
SysMon installed on SWIFT-connected systems

February 5 (AM):
Bank's printers go down

Mid-January 2016:
Attackers break into the network

February 4:
Attackers steal credentials of SWIFT users

February 5 (PM):
Fraudulent transactions sent

CYBERARK

The End Results

$81 million stolen and unrecovered

Millions laundered through casinos

Central bank governor **resigns**

Security **investigator missing** for six days

CYBERARK®

Background: What is SWIFT?

Member-owned co-op that enables central banks to securely send and receive monetary transactions

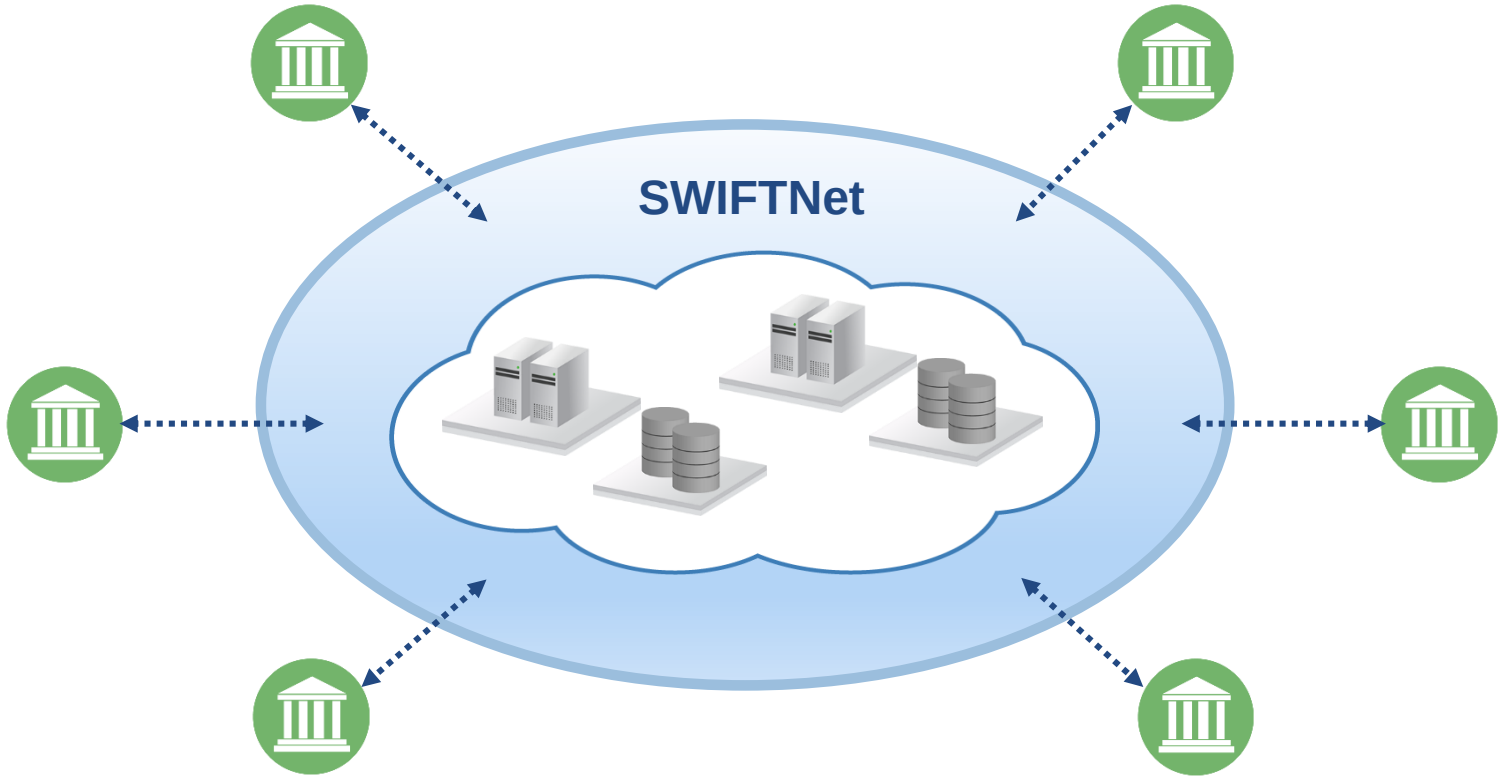
6.1+ billion
FIN messages

99.999%
SWIFTNet availability

99.999%
FIN availability

11,000+
Institutions connected to SWIFT

200+
Countries & territories connected



CYBERARK

SWIFT: Built for security

But only as strong as its weakest link

1. Authorized users receive digital certificates

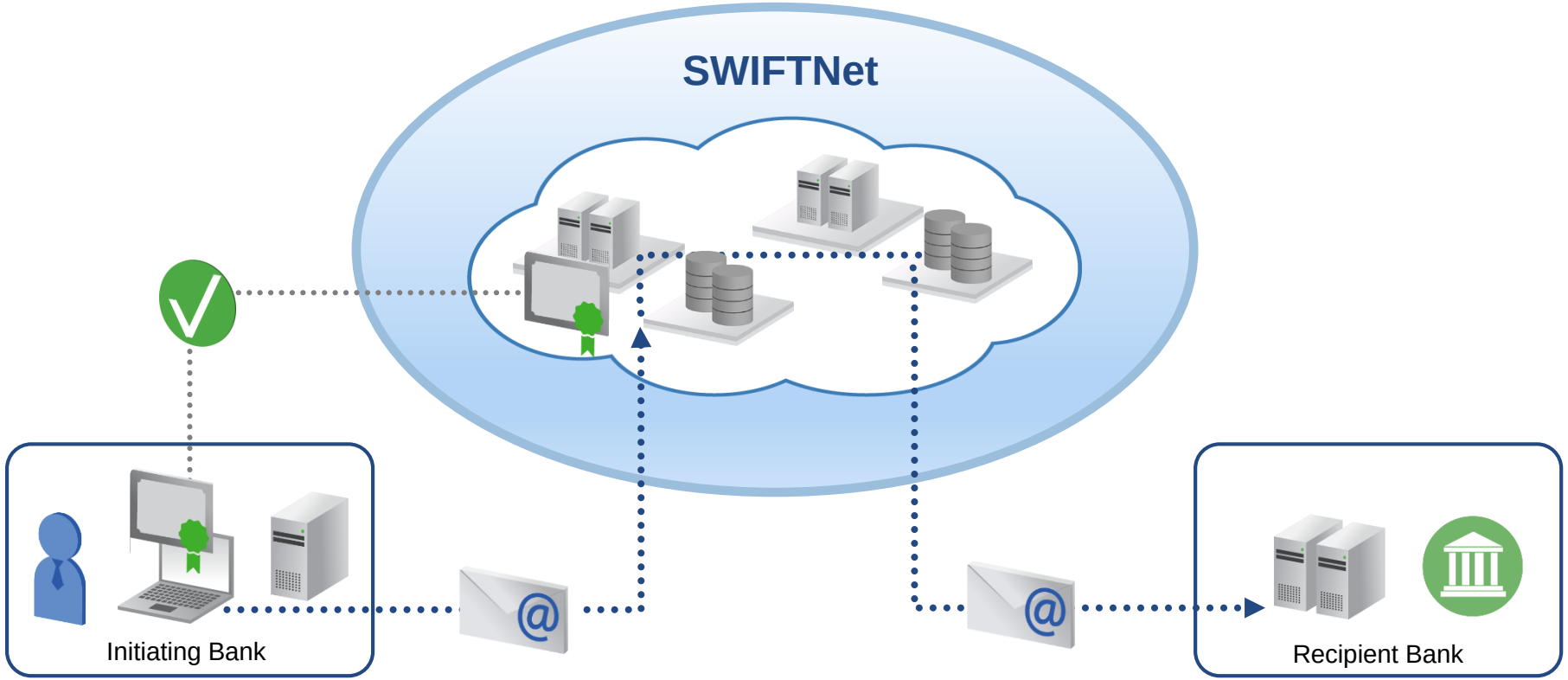
   ACCESS CONTROL

2. SWIFT validates certificates before sending messages

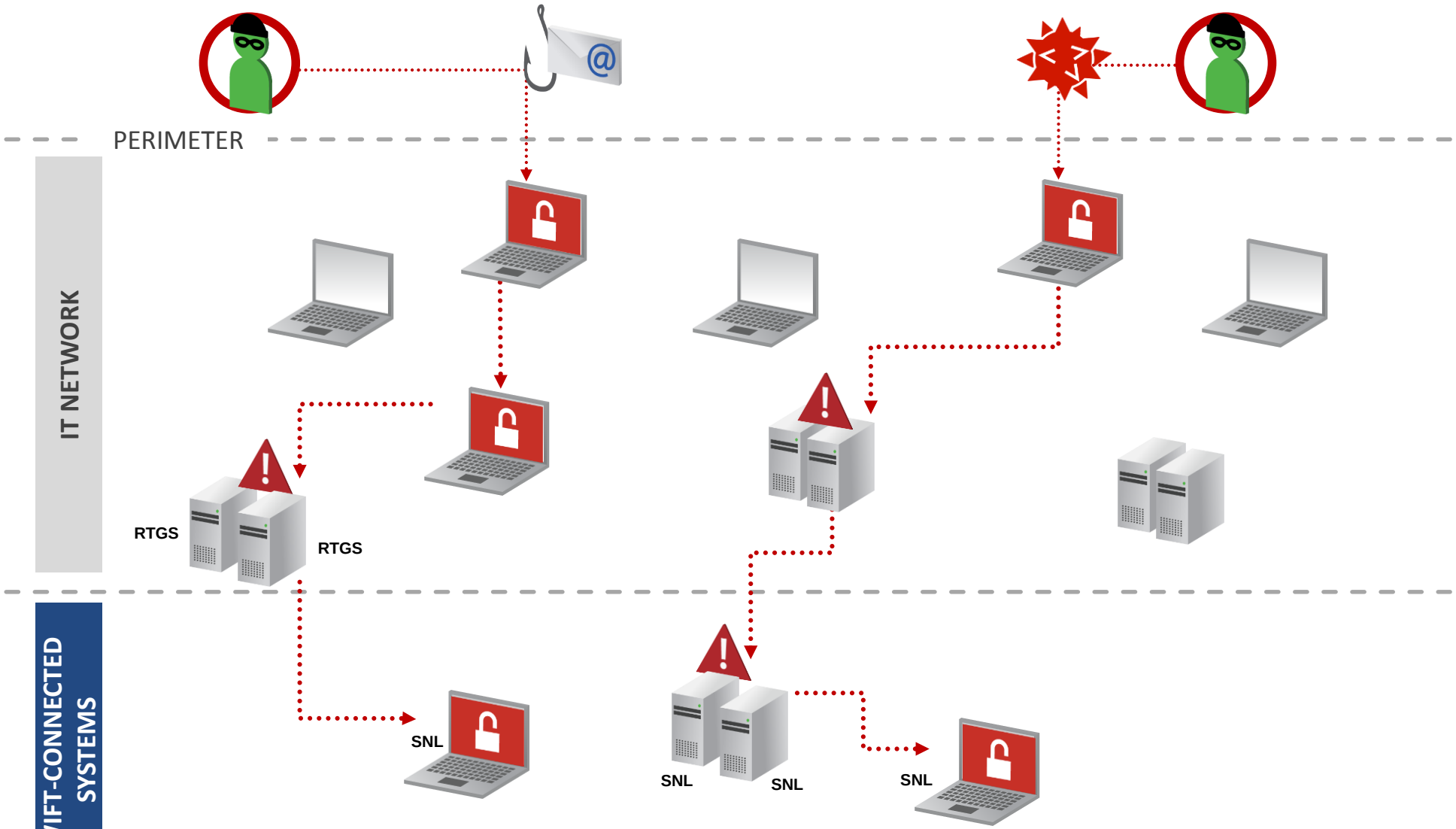
   AUTHENTICATION

3. Once validated, messages are securely sent to recipients

   ENCRYPTION

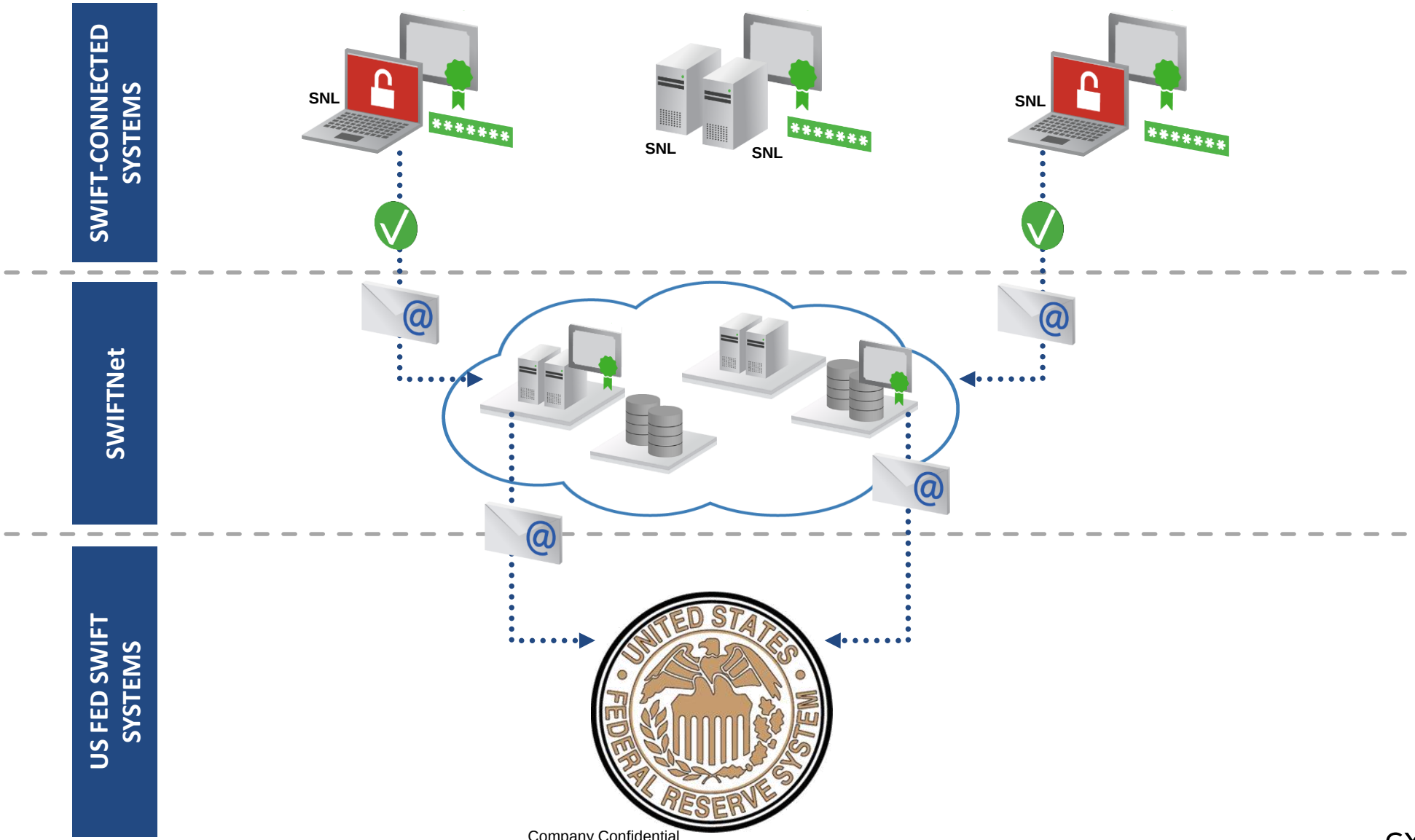


The pathway into SWIFTNet starts at the perimeter



CYBERARK®

Privileged exploits enable a cyber bank robbery



CYBERARK®

The damage could have been far worse

35 ORDERS WORTH **$951 MILLION** WERE SENT

5 ORDERS WORTH $101 MILLION WERE EXECUTED BY THE NY FED

$20 million transferred to Pan Asia Banking Company

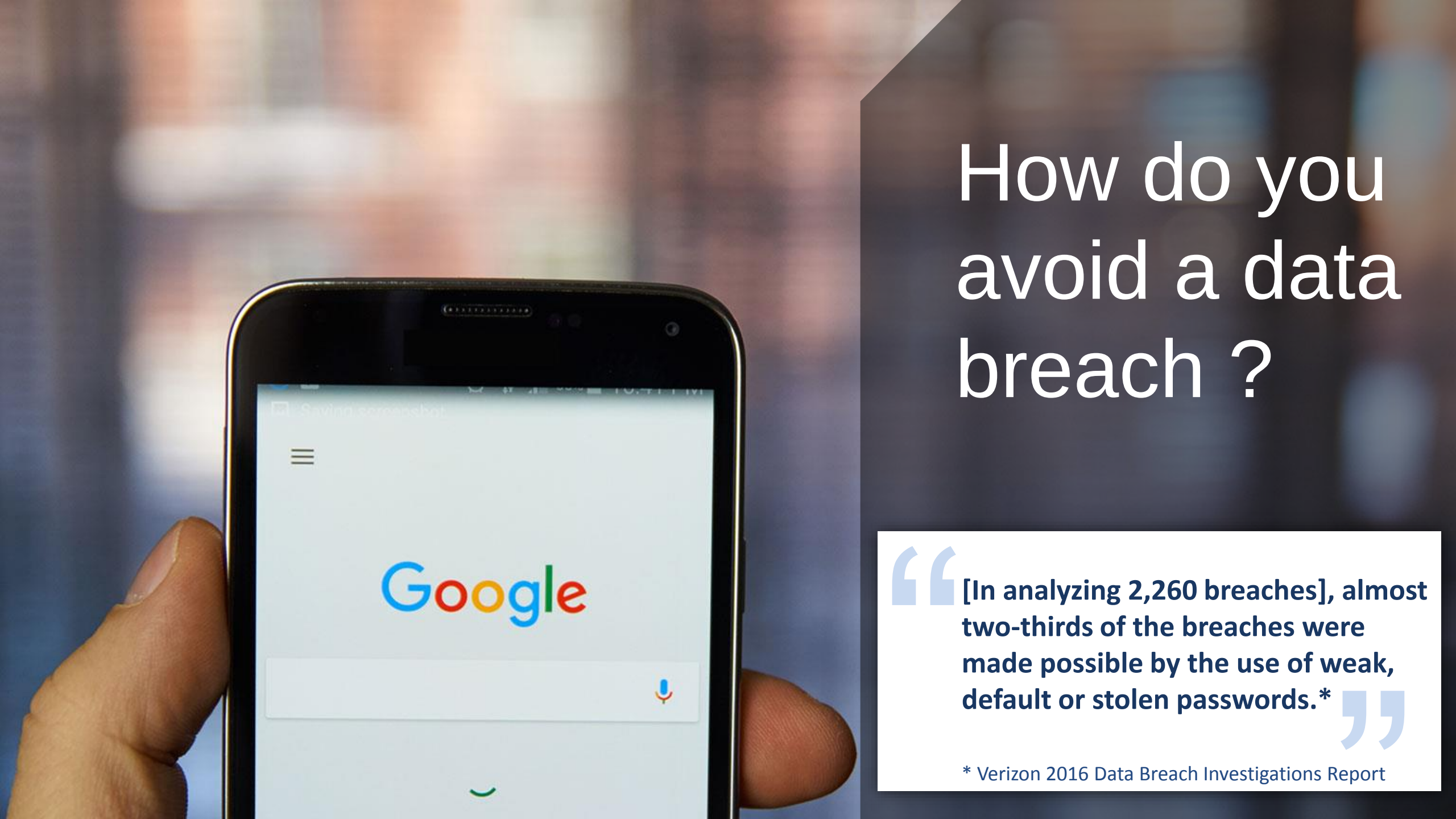
- $20 million stopped en route to “Shalika Fandation”

$81 million transferred to RCBC in the Philippines

- $29 million sent to hotel company
- $31 million delivered in cash to a guest of the hotel
- $21 million sent to a leisure company

30 ORDERS WORTH $850 MILLION WERE BLOCKED DUE TO A SUSPICIOUS RECIPIENT

CYBERARK®



How do you avoid a data breach ?

> **[In analyzing 2,260 breaches], almost two-thirds of the breaches were made possible by the use of weak, default or stolen passwords.***

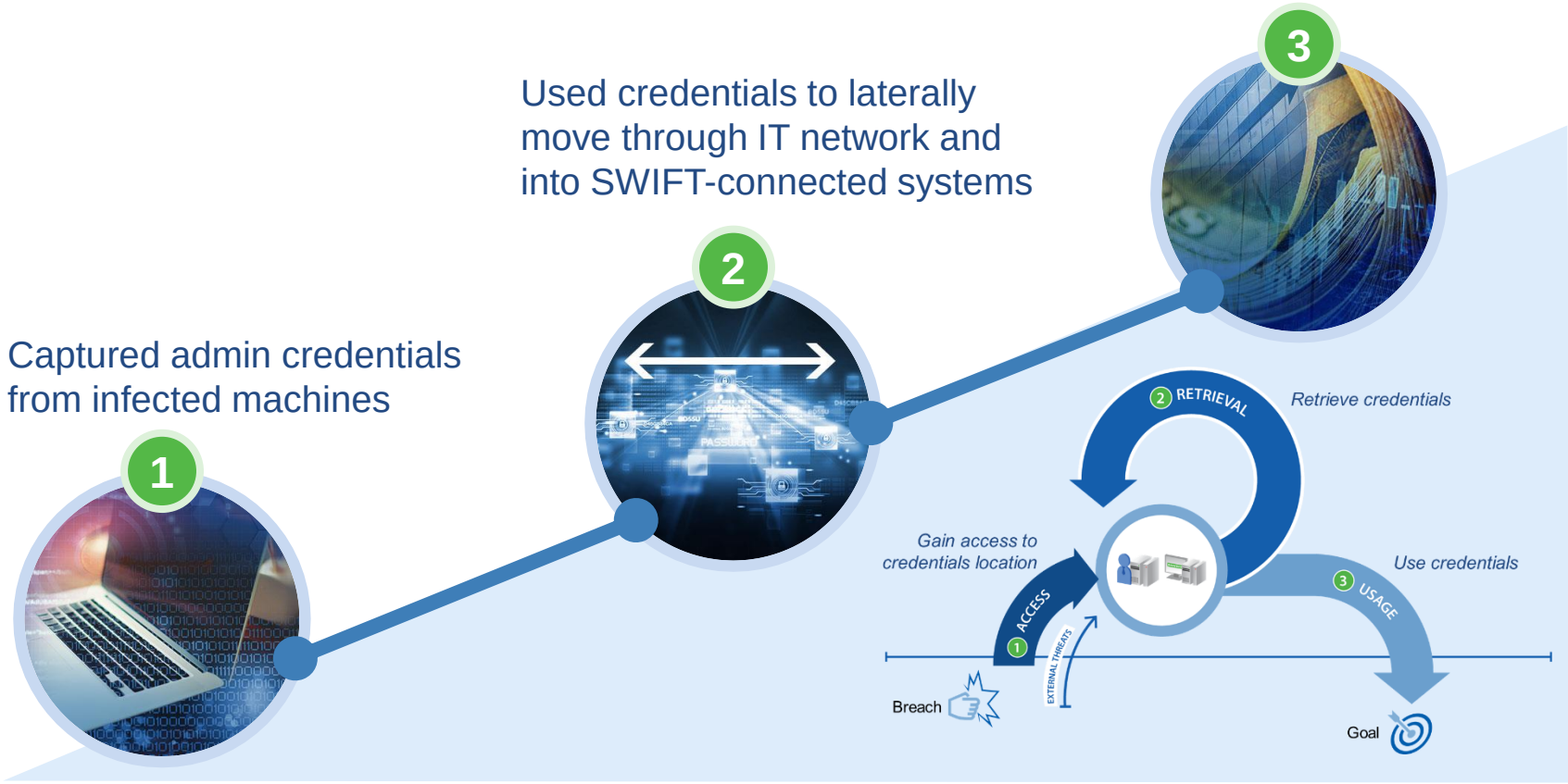
* Verizon 2016 Data Breach Investigations Report

The Role of Privilege in the Bangladesh Bank Heist

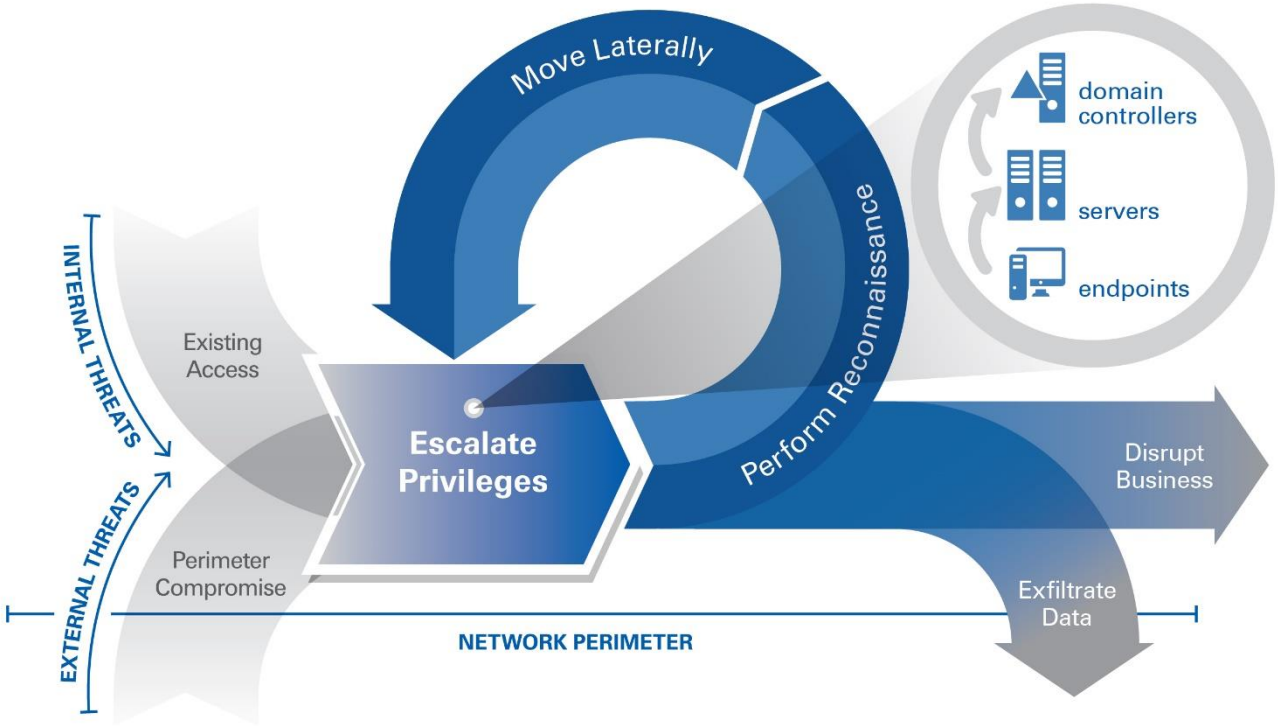
Captured admin credentials from infected machines

Used credentials to laterally move through IT network and into SWIFT-connected systems

Used compromised accounts to execute 35 financial transactions and cover tracks



We have to think like an attacker



First 3 Steps

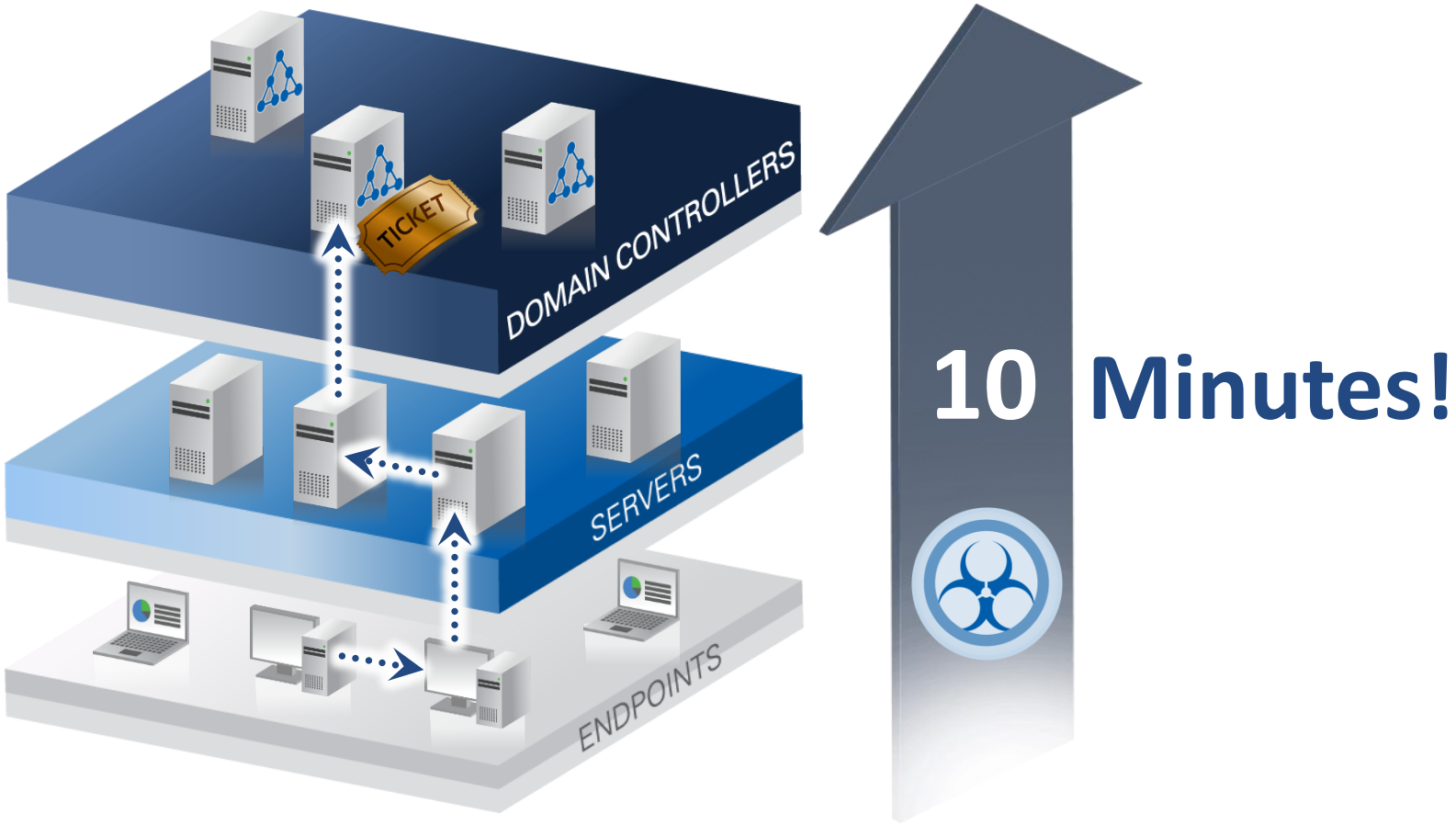
ATTACKER'S MINDSET:

1) Establish persistence in an organization by performing an attack that is not only hard to identify but also so intrusive that the business must rebuild to remove the attacker, e.g., a Kerberos attack such as a Golden ticket

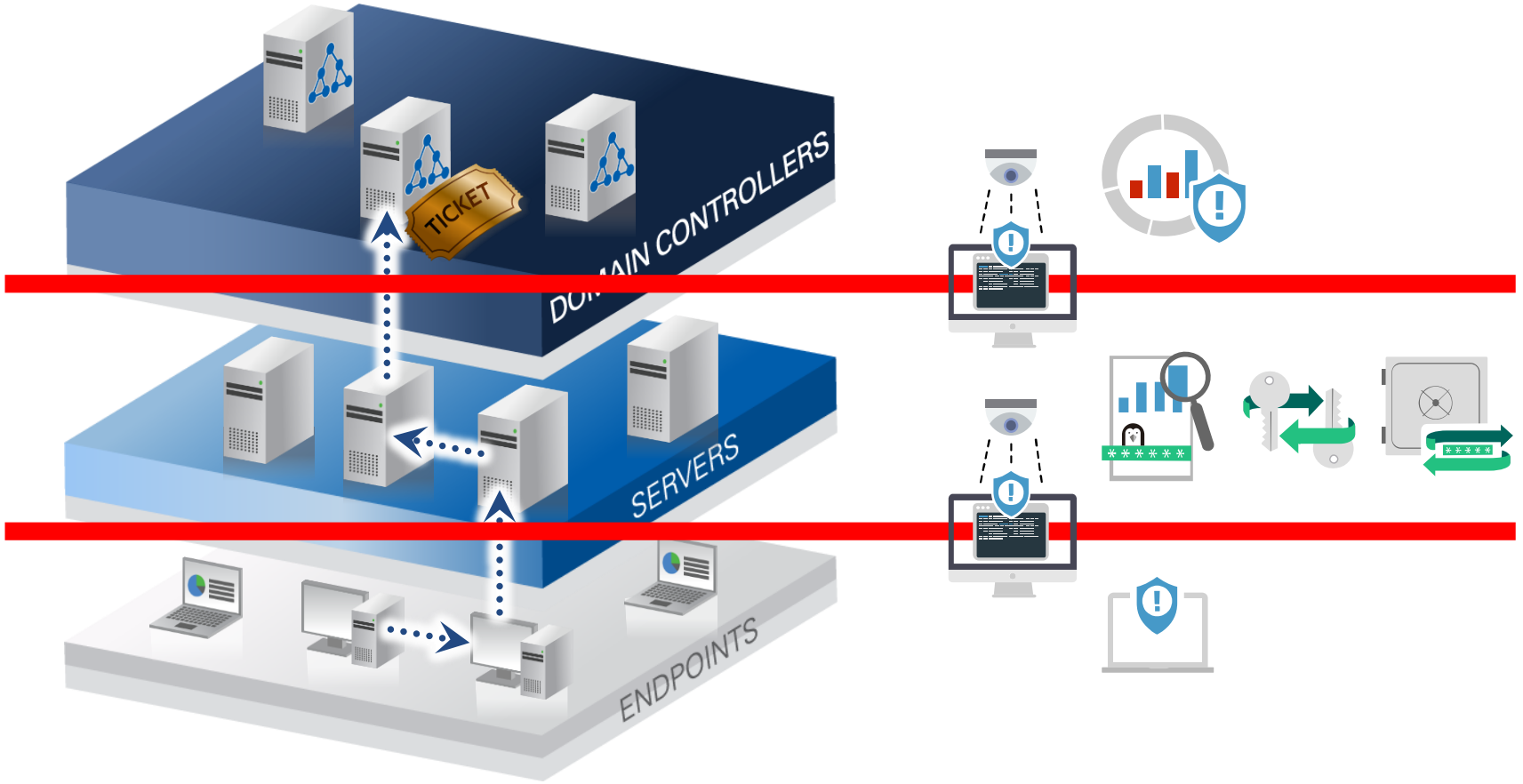
2) Take ownership of an entire technology stack by compromising a single infrastructure account, and use the same credentials on similar assets

3) Stealing credentials and moving laterally to IT Windows workstation in order to steal elevated permissions.

The Privileged Pathway



The Privileged Pathway



Key finding:

Attackers exploited vulnerabilities with Windows admin credentials

CYBERARK

Common practices that make organizations susceptible to attack

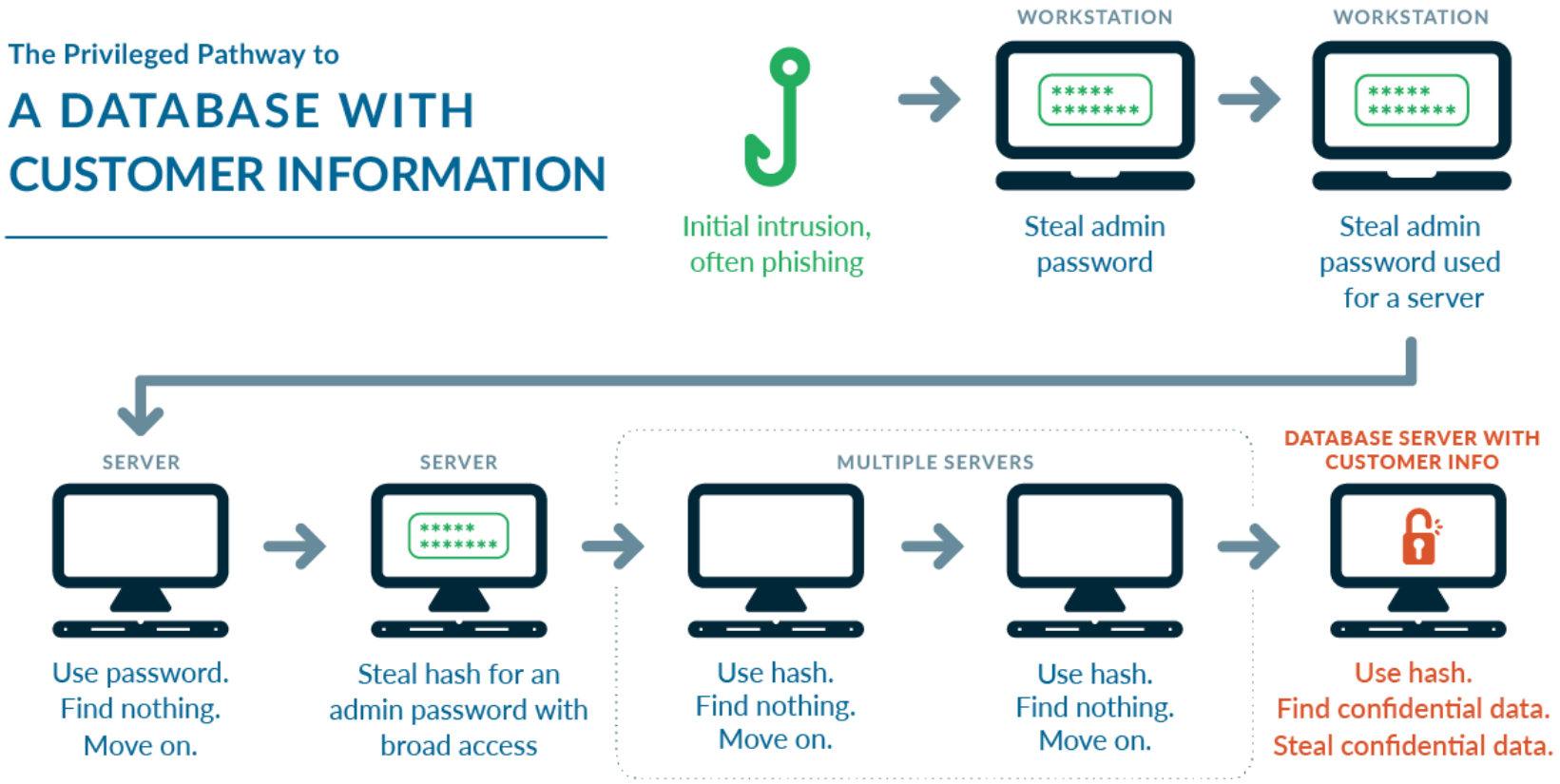
- Providing **end users with local admin rights** on their workstations
- Having **IT helpdesk staff use domain admin** accounts for troubleshooting
- Giving **IT admins access to domain admin** accounts, "just in case"
- Setting up **new workstations with cloned images**, all with the same local password
- Rotating administrator passwords **only every 30-60 days**
- Using an **AD Group Policy to rotate one administrative password** used for all machines
- Allowing accounts used by **applications to have domain administrator privileges**

> **Because many existing implementations of Active Directory Domain Services have been operating for years at risk of credential theft, organizations should assume breach and consider the very real possibility that they may have an undetected compromise of domain or enterprise administrator credentials.**

Microsoft, "Mitigating Pass-The-Hash and other Credential Theft, Version 2," 2014

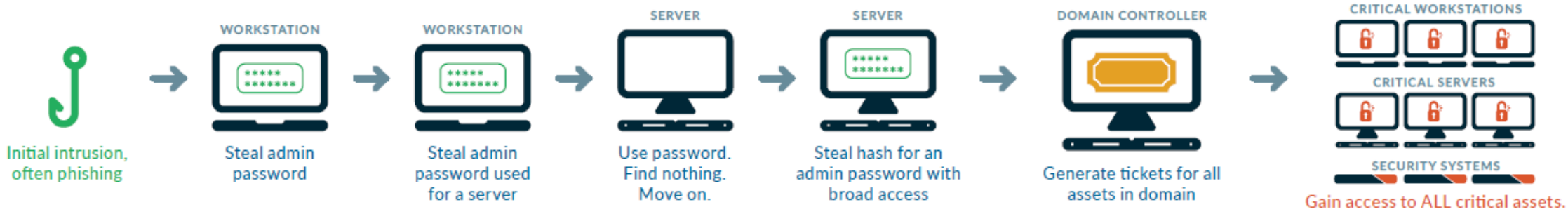
Key finding:

Attackers used a Privileged Pathway to get to critical assets



Key finding:

Attackers used a Privileged Pathway to get to critical assets



Common practices that leave organizations wide open to pass-the-hash and similar techniques include

- Permitting users to use accounts with **administrative privileges on their own workstations**
- Using the **same administrator password for all** local administrator accounts
- **Not** consistently **enforcing password rotation or uniqueness policies** for IT administrator accounts
- Setting up **domain administrator accounts** to be used **to log into to** domain controllers as well as **servers and workstations**
- Allowing **administrator accounts to be used for day-to-day tasks** such as checking email and browsing the Internet

CYBER-Hygiene Program

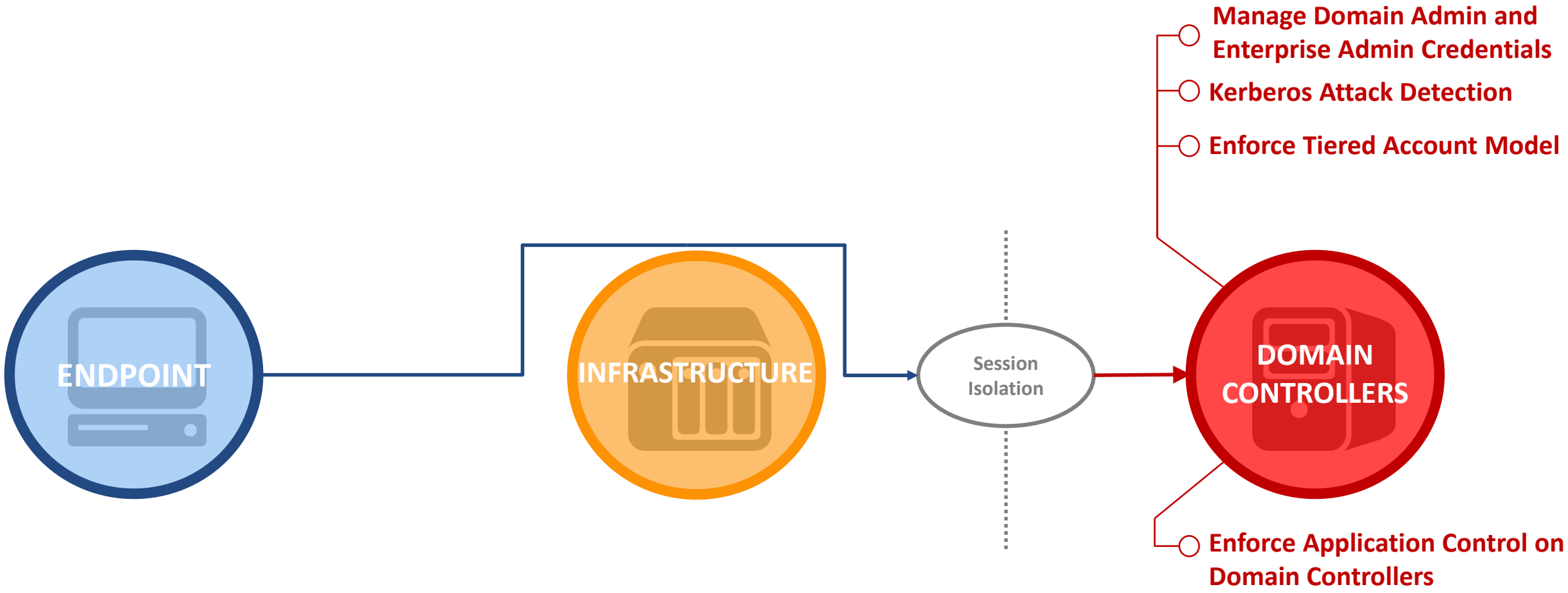
- Outlines the seven basic steps every PAS program should address over time
- Developed based on CyberArk's engagement with thousands of customers who embarked on PAS projects driven by:
  - Proactive project
  - Audit finding
  - Compliance requirement
  - Post-Breach remediation
- Focuses on steps that reduce the most risk relative to the level of resources and effort

18

PAS Hygiene Program Goals

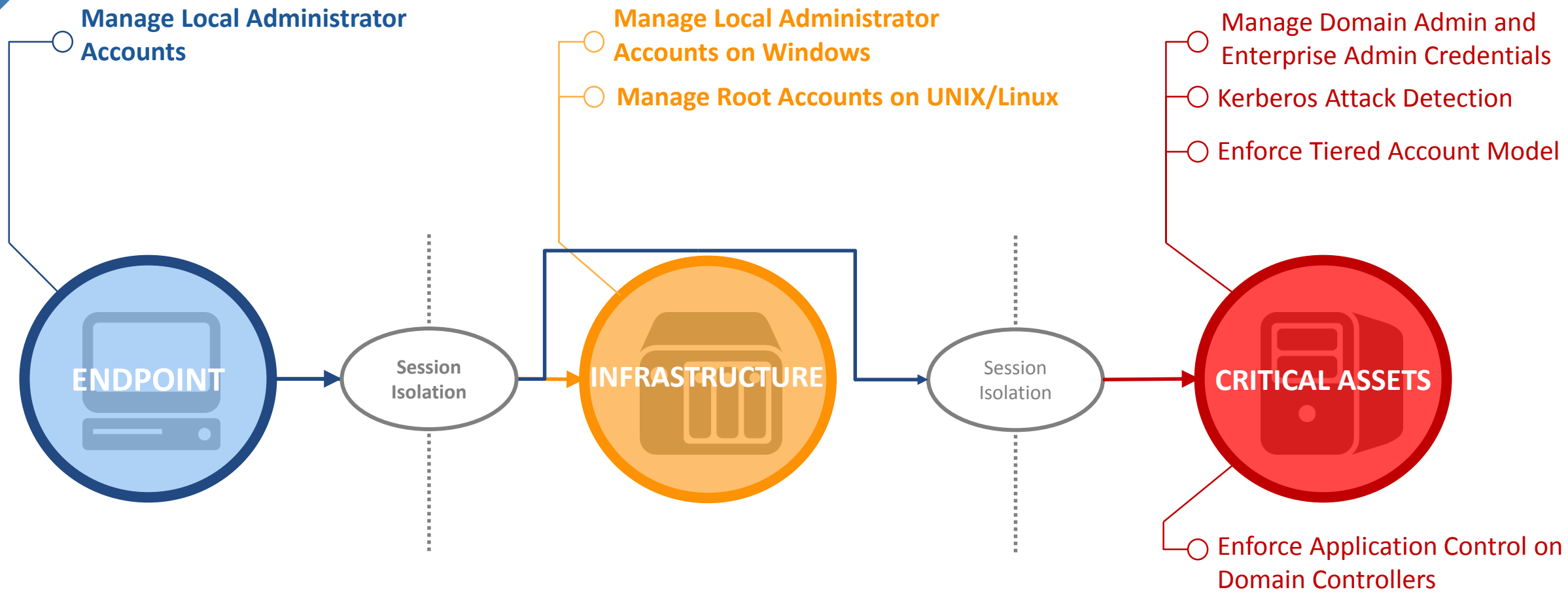
Step 1	Focus first on eliminating irreversible network takeover attacks (e.g., Kerberos Golden Ticket).
Step 2	Control & secure well-known infrastructure accounts.
Step 3	Limit lateral movement.
Step 4	Protect 3rd party privileged accounts.
Step 5	Manage SSH keys on critical Unix servers.
Step 6	Defend cloud & DevOps processes accounts.
Step 7	Secure shared IDs for business users (integrate and accelerate adoption of MFA).

1 Step 1: Irreversible Network Takeover Attacks



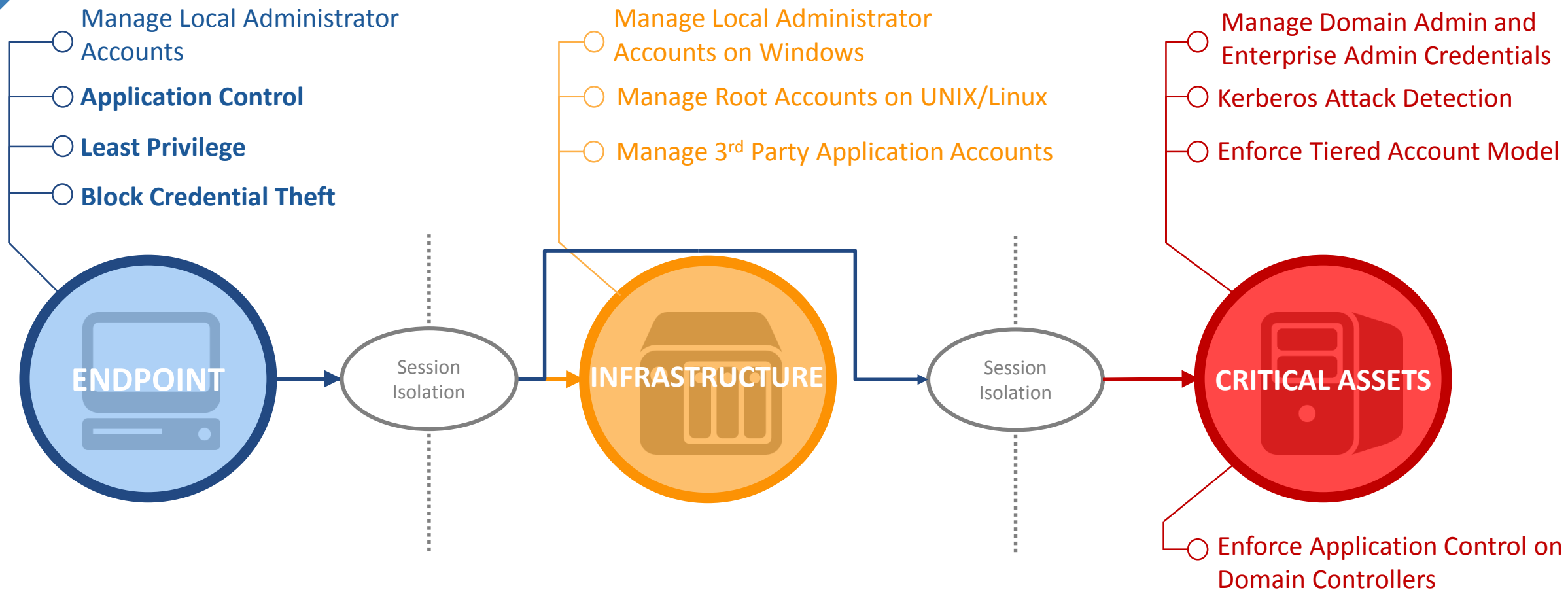
2

Step Two: Control & Secure Infrastructure and End Point Well-known Infrastructure Accounts



3

Step Three: Limit Lateral Movement



We have to think like the attacker

Look for exposed privileged accounts

- Exposed credentials alerts
- Unconstrained delegation alerts

Bypass Privileged Account Security controls

- Suspected credential theft
- Unmanaged privileged account

Known attacks for bypassing authentication

- Golden Ticket detection
- Overpass the Hash detection
- Hijacking Domain Accounts (DC Sync)

Go undetected while abusing privileged access

- Unusual access patterns
- Suspicious/risky privileged activity


CYBERARK
Thank You
Andrea.Argentin@CyberArk.com
PRIVILEGE
cyber attack
ON THE FRONT LINES